

REMARKS

Claims 1-17 are currently pending in the application; with claims 1, 9, and 13 being independent. Claims 2, 4, and 10 were amended to address minor informalities. Applicants have added new claims 13-17 to define additional aspects of the invention. Applicants request favorable consideration in light of the comments and amendments presented herein, and earnestly seek timely allowance of the pending claims.

Allowable Subject Matter

The Examiner indicated that claim 6 was directed to allowable subject matter, but was objected to as depending from a rejected base claim. Applicants wish to thank the Examiner for the indication of allowable subject matter.

Information Disclosure Statement

In the outstanding Office Action, the Examiner returned the form PTO-1449 with an indication that the document "Security Measures Handled by Specialists," Nikkei Communications 9/20, 1999, Feature 94, was not considered because it was not provided in the Information Disclosure Statement. Applicants submit that this reference was supplied with the Information Disclosure Statement, and believe that an inadvertent scanning error bundled this reference with another reference submitted in the IDS, making it appear that it was not provided. For the convenience of the Examiner, Applicants supply herewith another copy of this reference.

Applicants respectfully request the Examiner consider this reference and supply another copy of the form PTO-1449 indicating said consideration.

Claim Objections

In the outstanding Office Action, the Examiner objected to claims 2 and 10 because they contained informalities. Specifically, the Examiner asserted that in line 7 of claim 2 and in line 6

of claim 10, the word “communication” was misspelled. Applicants have amended claims 2 and 10 to correct these informalities.

Claim Rejections – 35 USC §112

The Examiner rejected claim 4 under 35 USC §112, second paragraph, as being indefinite. Specifically, the Examiner asserts that the recitation “reception section receives an encapsulated illegal access data by the illegal access data detection device from the illegal access data detection device” is unclear. Applicants have amended claim 4 and respectfully request the Examiner withdraw the §112, second paragraph, rejection.

Claim Rejections – 35 USC §102

The Examiner rejected claims 1-3 and 9-11 under 35 USC 102(e) as being anticipated by US Patent No. 6, 678,827 to Rothermel et al. (“Rothermel”). Applicants submit the Examiner failed to establish a *prima facie* case of anticipation and traverse this rejection.

Rothermel merely discloses a way to remotely manage multiple network security devices. Specifically, Rothermel discloses utilizing network security devices (NSD), which attempt to control the spread of sensitive information so that only authorized users or devices can retrieve such information. Such types of NSDs, such as firewalls and security appliances, have a group of one or more trusted network devices which the NSD attempts to protect from unauthorized external access (col. 1, lines 23-30). The NSD monitor network information passing between external network devices and the devices in their group of trusted or internal devices (col. 1, lines 30-33).

As shown in Fig. 1, the network security device management system includes a security policy manager device 110 able to communicate with multiple superior devices 120 and 160, also referred to as host devices or event processor. Each supervisor device is associated with multiple NSDs, with supervisor device 120 associated with NSDs 130-140, and with supervisor device 160 associated with NSDs 161-162. Each NSD protects one or more trusted devices from external devices, such as NSDs 130 and 140 protecting devices (not shown) in internal networks 135 and 145, respectively, from devices (not shown) an external network 190.

However, Rothermel fails to disclose, at least, “an illegal access data handling device, being placed outside a given internal communications network,” as recited in claim 1 (emphasis added), and “a method for handling illegal access data outside a given internal communication network,...receiving illegal access data transmitted from a data communication device placed outside the internal communications network,” as recited in claim 9.

As indicated in the Office Action, the Examiner asserts that the network security device management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus. Rothermel merely discloses that NSDs within the network security device management system can protect trusted devices from other devices reciting on either internal or external networks. However, Rothermel fails to disclose that the network security device management system is placed outside an internal communications network.

Accordingly, Applicants respectfully request the Examiner to withdraw the rejection of independent claims 1 and 9. Claims 2-3 depend from claim 1 and are allowable at least by virtue of their dependency, and claims 10-11 depend from claim 9, and are allowable at least by virtue of their dependency from allowable claim 11.

Claim Rejections – 35 USC §103

The Examiner rejected claims 4, 7, and 8 under 35 USC 103(a) as being unpatentable over Rothermel in view of US Patent No. 6,321,337 to Reshef et al. (“Reshef”). Applicants submit the Examiner has failed to establish a *prima facie* case of obviousness, and traverse this rejection.

Claims 4, 7, and 8 depend from claim 1 and include all the recitations provided therein by virtue of their dependency.

Reshef merely discloses a security gateway system acting as an intermediary between a trusted computing environment and an untrusted computing environment, and thus fails to cure the deficiencies of Rothermel as provided above in the arguments for the allowability of claims 1 and 9.

Accordingly, Applicants respectfully request the Examiner withdraw the rejection of claims 4, 7, and 8.

The Examiner rejected claims 5 and 12 under 35 USC 103(a) as being unpatentable over Rothermel in view of US Patent No. 6,826,697 to Moran ("Moran"). Applicants disagree and respectfully traverse the rejection.

Claim 5 depends from claim 1, and claim 12 depends from claim 9, and accordingly include all of the recitations provided in the respective independent claims by virtue of their dependency.

Moran merely teaches a system and method for detecting intrusions in a host system on a network. The intrusion detection system comprises an analysis engine configured to use continuations and apply forward- and backward chaining using rules.

Moran fails to cure the deficiencies of Rothermel as provided above and the arguments for the allowability of claims 1 and 9.

Accordingly, Applicants respectfully request the Examiner to withdraw the 103 rejections of claims 5 and 12.

Conclusion

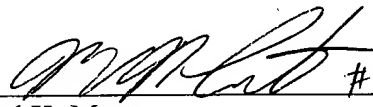
In view of the above amendments and remarks, this application appears to be in condition for allowance and the Examiner is, therefore, requested to reexamine the application and pass the claims to issue.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact the undersigned at telephone number (703) 205-8000, which is located in the Washington, DC area.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Date: November 10, 2005

Respectfully submitted,

By  #39,491
for Michael K. Mutter
Registration No.: 29,680
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Rd
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant

Attachment: Copy of "Security Measures Handled by Specialists," Nikkei Communications
9/20, 1999, Feature 94 (3 pages)
Copy of PTO-1449 Form dated 11/12/02